M2 informatique
Année universitaire 2018-2019 - Session 2

Consignes : Les documents sont interdits. Les calculatrices et téléphones portables sont interdits.

Examen d'administration réseau

Exercice 1 – Adressage et NAT (7 points)

Nous supposons un réseau d'entreprise d'adressage privé statique 10.0.0.* et disposant d'un routeur A. A est connecté à un équipement B appartenant au fournisseur d'accès à Internet de l'entreprise. A obtient une adresse privée dynamique 192.168.1.* de B. B est relié à Internet.

Question 1.1 (1 point) : Représentez graphiquement l'architecture.

Question 1.2 (1 point) : Quelles sont les adresses IP des routeurs A, B et d'un utilisateur du réseau privé ?

Question 1.3 (1 point) : Rappelez le fonctionnement de DHCP. Quels équipements l'utilisent ?

Question 1.4 (2 points) : Comment configurer le réseau pour qu'un internaute puisse accéder à un serveur du réseau privé ? Illustrez la transmission d'un paquet IP de l'internaute au serveur, en indiquant systématiquement l'adresse destination.

Question 1.5 (2 points) : Quels sont les avantages du NAT lorsque l'on utilise un adressage statique ?

Exercice 2 – Architecture réseau (10 points)

Vous êtes le responsible réseau d'une pépinière d'entreprises dans le domaine des services web. La pépinière héberge plusieurs entreprises simultanément, chacune pour une durée d'un an maximum. La pépinière dispose d'une trentaine de bureaux pouvant accueillir trois personnes chacun.

Question 2.1 (1 point) : Décrivez votre politique d'affectation des bureaux aux entreprises.

Question 2.2 (1 point) : Décrivez une architecture réseau simple permettant de gérer la pépinière. Vous insisterez sur le type et la quantité de matériel réseau utilisé, en justifiant vos choix. Vous pouvez faire un schéma.

En tant que responsable réseau, vous êtes tenu de garantir la connectivité à Internet aux employés des entreprises. Vous disposez de deux connexions à Internet, chacune ayant une connectivité garantie pendant 99% du temps (sous peine de vous dédommager).

Question 2.3 (2 points) : Comment augmenter la robustesse de votre réseau interne ? Indiquez les conséquences sur la topologie du réseau et sur le matériel. Quels sont les protocoles à configurer pour prendre en compte cette robustesse ?

Question 2.4 (2 points) : Par rapport aux entreprises hébergées, à quoi pouvez-vous vous engager par rapport à la garantie de connectivité à Internet ? Justifiez le dédommagement que vous proposez de fournir aux entreprises si vous ne pouvez pas tenir vos engagements.

Question 2.5 (1 point) : Comment pouvez-vous mesurer le temps pendant lequel la connectivité à Internet est impossible ?

Question 2.6 (1 point) : Comment différencier une panne de DNS d'une panne de connectivité à Internet ?

Question 2.7 (2 points) : Chaque entreprise possède des serveurs web publics. Comment procéder pour rendre ces serveurs web indépendants, de manière à ce qu'une faille d'un serveur d'une entreprise donnée n'affecte pas les serveurs des autres entreprises ? Pour des raisons d'utilisabilité, tous les serveurs se trouvent physiquement proches.

Exercice 3 – Décodage de trames (3 points)

Question 3.1 (3 points) : On récupère la trame suivante sur le réseau via le sniffer Wireshark. Quelles informations contient-elle ? Analysez la trame afin de récupérer les différents protocoles encapsulés et les données des émetteurs et destinataires.

```
40 b9 3c bf aa 6f 98 90  96 a2 69 0d 08 00 45 00
00 38 27 66 00 00 80 11  02 49 ac 10 40 03 c0 a8
64 4a f0 01 00 35 00 24  4f 62 99 4f 01 00 00 01
00 00 00 00 00 00 06 65  63 6f 73 69 61 03 6f 72
67 00 00 01 00 01
```

Pour rappel :

Format d'une trame PDU-Ethernet II ou PDU-802.3 :

Destination (6)	Source (6)	Type/longueur (2)	Données (<1500)	Bourrage (<46)

Champ type/longueur :

- 0000 à 05DC = longueur IEEE 802.3
- 0800 = IP
- 0806 = ARP
- 0808 = Frame Relay ARP

Format d'une trape IP :

Version (4 bits)	Longueur entête sur 4 (4 bits)	Service QoS (1)	Longueur totale (2)	
Identifiant du fragment (2)			Drapeau (3 bits)	Position du fragment (13 bits)
TTL (1)		Protocole encapsulé (1)	Checksum (2)	
Adresse IP source (4)				
Adresse IP destination (4)				

Données (variable)

Drapeaux : 010 = autorisation de fragmentation, 001 = dernier fragment
Protocole encapsulé : 1 = ICMP, 6 = TCP, 17 = UDP

Format d'une trame TCP :

Port source (2)		Port destination (2)
Numéro de séquence (4)		
Numéro d'acquittement (4)		
Longueur entête (3 bits)	Flags TCP (13 bits)	Fenêtre TCP (2)
Checksum TCP (2)		Pointeur urgent (2)
Options TCP (variable)		
Données (variable)		

Flags TCP :

- 0000000100000 = URG
- 0000000010000 = ACK
- 0000000001000 = PSH
- 0000000000100 = RST
- 0000000000010 = SYN
- 0000000000001 = FIN

Format d'une trame UDP :

Port source (2)	Port destination (2)
Taille des données (2)	Checksum UDP (2)
Données (variable)	

Format d'une trame DNS :

Transaction ID (2)	Flags (2)	Nombre questions (2)	Nombre réponses RR (2)
Nombre d'autority RR (2)	Nombre d'additional RR (2)	Nom de l'hôte - zone 2 (variable)	
Type zone 2 (2)	Classe zone 2 (2)	Réponse - zone 3 (variable)	
Type zone 3 (2)	Classe zone 3 (2)	TTL réponse (4)	
Longueur adresse réponse (2)	Adresse recherchée (variable)	Nom des serveurs faisant autorité – zone 4 (variable)	
Options zone 4 (variable)		Enregistrements additionnels – zone 5 (variable)	
Options zone 5 (variable)			